Claims

1. A method for allowing a predetermined access to at least a subset of a software application, the method comprising the steps of:

   calculating an identifier based at least in part on a user file;

   generating an access key based at least in part on the identifier; and

   validating the access key against a user data key and, on successful validation, granting the predetermined access to the at least a subset of the software application.

2. The method of claim 1 further comprising the step of executing an activation routine on unsuccessful validation.

3. The method of claim 1 wherein the predetermined access comprises run permitted access.

4. The method of claim 1 wherein the user file comprises input data for the software application.

5. The method of claim 1 wherein the identifier comprises a checksum based at least in part on a cyclic redundancy check.

6. The method of claim 1 wherein the user file includes at least one file characteristic.

7. The method of claim 6 wherein the at least one file characteristic comprises at least one of an element count, a node count, a model name, and a match ratio.

8. The method of claim 6 wherein the access key further comprises the at least one file characteristic.

9. The method of claim 1 wherein the access key further comprises a software application signature.

10. The method of claim 1 wherein the access key further comprises at least one system characteristic.

11. The method of claim 1 wherein the access key is encrypted.

12. The method of claim 1 wherein the access key has a limited validity lifetime.

13. The method of claim 12 wherein the limited validity lifetime is determined at least in part by at least one of an elapsed time from access key generation, a number of access key validations, and a frequency of access key validations.

14. The method of claim 1 wherein the user data key comprises a previously calculated result based at least in part on the user file.

15. A method of creating a user data key for a software application, the method comprising the steps of:

receiving an identifier based at least in part on a user file;

including the identifier in a fingerprint;

encrypting the fingerprint; and

associating the fingerprint with the software application as the user data key.

16. The method of claim 15 wherein the user file comprises input data for the software application.

17. The method of claim 15 wherein the identifier comprises a checksum based at least in part on a cyclic redundancy check.

18. The method of claim 15 wherein the user file includes at least one file characteristic.

19. The method of claim 18 wherein the at least one file characteristic comprises at least one of an element count, a node count, a model name, and a match ratio.

20. The method of claim 18 wherein the fingerprint comprises the at least one file characteristic.

21. The method of claim 15 wherein the fingerprint comprises a software application signature.

22. The method of claim 15 wherein the fingerprint comprises at least one system characteristic.

23. The method of claim 15 further comprising the step of receiving payment associated with the user data key.

24. The method of claim 23 wherein the step of receiving payment comprises a credit card transaction.

25. The method of claim 23 wherein the step of receiving payment comprises a coupon transaction.

26. The method of claim 15 wherein the step of associating the fingerprint with the software application further comprises transmitting the fingerprint to the software application.

27. The method of claim 26 wherein the user data key is included in a dynamic link library file.

28. A network enabled application software distribution method including the steps of:

providing a restricted use application software program;

loading the program onto a user's computer;

establishing communications between the user's computer and another computer;

uploading a fingerprint file from the user's computer to the other computer;

downloading a key file from the other computer to the user's computer; and

running the application software program on the user's computer.

29. A method for allowing a run permitted access to at least a subset of a software application, the method comprising the steps of:

calculating an identifier based at least in part on a user file, the user file including input data for the software application and having at least one file characteristic, and the identifier including a checksum based at least in part on a cyclic redundancy check;

generating an access key based at least in part on at least one of the identifier, the at least one file characteristic, a software application signature, and at least one system characteristic;

encrypting the access key; and

validating the access key against a user data key that includes a previously calculated result based at least in part on the user file and, on successful validation, granting the predetermined access to the at least a subset of the software application and, on unsuccessful validation, executing an activation routine.

30. The method of claim 29 wherein the at least one file characteristic comprises at least one of an element count, a node count, a model name, and a match ratio.

31. The method of claim 29 wherein the access key has a limited validity lifetime.

32. The method of claim 31 wherein the limited validity lifetime is determined at least in part by at least one of an elapsed time from access key generation, a number of access key validations, and a frequency of access key validations.

33. A method of creating a user data key for a software application, the method comprising the steps of:

receiving an identifier based at least in part on a user file, the user file having input data for the software application and having at least one file characteristic, and the identifier including a checksum based at least in part on a cyclic redundancy check;

including the identifier in a fingerprint, the fingerprint including at least one of the at least one file characteristic, a software application signature, and at least one system characteristic;

encrypting the fingerprint; and

associating the fingerprint with the software application as the user data key by transmitting the fingerprint to the software application, and by using a dynamic link library file, and in response to receiving payment.

34. The method of claim 33 wherein the at least one file characteristic comprises at least one of an element count, a node count, a model name, and a match ratio.

35. The method of claim 33 wherein receiving payment comprises a credit card transaction.

36. The method of claim 33 wherein receiving payment comprises a coupon transaction.

37. A software access control apparatus comprising:

an identifier calculator in communication with a user file;

an access key generator in communication with the identifier calculator; and

a validator in communication with the access key generator and a user data key.

38. A user data key generator comprising:

an identifier receiver;

a fingerprint compiler in communication with the identifier receiver;

an encryption engine in communication with the fingerprint compiler; and

a transmitter in communication with the encryption engine and a software application.

39. A computer system for allowing a predetermined access to at least a subset of a software application comprising:

means for calculating an identifier based at least in part on a user file;

means for generating an access key based at least in part of the identifier;

means for encrypting the access key;

means for validating the access key against a user data key; and

means for granting the predetermined access in response to successful validation.

40. The computer system of claim 39 further comprising means for executing an activation routine in response to unsuccessful validation.

41. A computer system for creating a user data key for a software application comprising:

means for receiving an identifier based at least in part on a user file;

means for including the identifier in a fingerprint;

means for encrypting the fingerprint; and

means for associating the fingerprint with the software application as the user data key.

42. An article of manufacture comprising a program storage medium having computer readable program code embodied therein for allowing a predetermined access to at least a subset of a software application, the computer readable program code in the article of manufacture including:

computer readable code for causing a computer to calculate an identifier based at least in part on a user file;

computer readable code for causing a computer to generate an access key based at least in part on the identifier; and

computer readable code for causing a computer to validate the access key against a user data key and, on successful validation, grant the predetermined access to the at least a subset of the software application.

43. A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for allowing a predetermined access to at least a subset of a software application, the method steps comprising:

calculating an identifier based at least in part on a user file;

generating an access key based at least in part on the identifier; and

validating the access key against a user data key and, on successful validation, granting the predetermined access to the at least a subset of the software application.

44. An article of manufacture comprising a program storage medium having computer readable program code embodied therein for creating a user data key for a software application, the computer readable program code in the article of manufacture including:

computer readable code for causing a computer to receive an identifier based at least in part on a user file;

computer readable code for causing a computer to include the identifier in a fingerprint;

computer readable code for causing a computer to encrypt the fingerprint; and

computer readable code for causing a computer to associate the fingerprint with the software application as the user data key, so as to create the user data key.

45. A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for creating a user data key for a software application, the method steps comprising:

receiving an identifier based at least in part on a user file;

including the identifier in a fingerprint;

encrypting the fingerprint; and

associating the fingerprint with the software application as the user data key, so as to create the user data key.